PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of:

Inventor(s)	:	Leo Pedlow, Jr., et al.
Filed	:	4/13/2004
Serial No.	:	10/823,431
Confirmation No.	:	4023
Group Art Unit	:	2132
Examiner	:	Homayounmehr, Farid
Docket Number	:	SNY-T5775.02
Title	:	Composite Session Based encryption for Video On Demand Content

---

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING

I hereby certify that this correspondence is, on the date shown below, being deposited with the U.S. Postal Service as first class mail with sufficient postage in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Applicant, Assignee or Reg. Representative: JERRY A. MILLER Reg. No. 30,779

Signature: /Jerry A. Miller 30779/ Date: 9/18/2007

APPEAL BRIEF

This appeal brief is submitted in **triplicate** in response to the Office Action dated 6/21/2007. Reconsideration and allowance of all claims at issue are respectfully requested.

The fee for this brief is being paid by [X] credit card payment form [ ] check [ ] deducted from deposit account number 501267. The Commissioner is authorized to deduct any underpayment or credit any overpayment to deposit account number 501257.

REAL PARTY IN INTEREST

The real parties in interest in this appeal is the assignees of this application - Sony Corporation and Sony Electronics, Inc.

RELATED APPEALS AND INTERFERENCES

None known to the undersigned.

STATUS OF CLAIMS

Claims 1 – 6 and 8 - 33 are pending. Claims 1, 11, 18, 19, 24 and 30 are currently amended. Claim 7 has been canceled. Claims 1 – 6 and 8 – 33 stand rejected under 35 U.S.C. 103(a) as being unpatentable over So (US Patent Application Publication 2002/0083438) in view of Colligan (US Patent 6,415,031), both of record.

STATUS OF AMENDMENTS FILED SUBSEQUENT TO FINAL REJECTION

There are no current amendments filed subsequent to final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The following summary is supplied in compliance with the requirements of the appeal rules. The undersigned wishes to note that this summary is provided merely as an aid to the Board in rapidly understanding the invention and the issues relating to this appeal and do not supersede what the claims actually state (69 Fed, Reg, 155 (Ayg, 2004). Citations from the specification, drawings and reference numbers are intended to be illustrative. As such, this summary should not be construed to limit the invention in any way.

Claim Group 1

Claim 1 is representative of Claim Group 1 below. According to certain embodiments as characterized by claim 1, a Video On Demand (VOD) method provides session based selective encryption (e.g., page 6, line 27 through page 7, line 5, Fig. 2, item 104):

the method includes processing content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted (e.g., page 13, lines 5-9, Fig. 2, items 108 and 112);

storing the first portions and storing the second portions (e.g., page 13, lines 10-11 and page 14, line 21, Fig. 3, item 208);

receiving a request for delivery of the content from a subscriber terminal to initiate a VOD session (e.g., page 13, line 13, Fig. 3, item 212);

determining if the subscriber terminal has decryption capabilities associated with a first decryption method or a second decryption method (e.g., page 13, lines 14-15, Fig. 2, item 104);

if the request is from a subscriber terminal having decryption capabilities associated with the first decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the first decryption method to initiate a VOD session (e.g., page 13, lines 15-17, Fig. 3, item 216);

routing the first portions to a first encryption device that encrypts content for decryption under the first encryption method, to provide encryption of the first portions for the VOD session, and route the second portions around the first encryption device (e.g., page 14, lines 25-27, Fig. 3, item 222 and 226);

encrypting neither the first nor the second portions using a second encryption device that encrypts content for decryption under the second decryption method for the VOD session (e.g., page 11, lines 16-20, Fig. 2, item 104);

encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions (e.g., page 13, lines 19-20, Fig. 2, item 116);

if the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method, the first portions of content are routed to a second encryption device that encrypts content for decryption under the second encryption method and provides encryption of the first portions for the VOD sessions (e.g., page 13, lines 22-26, Fig. 2, item 124, 128, 132);

routing the second portions around the second encryption device, and encrypts neither the first nor the second portions using the first encryption device that encrypts content for decryption

under the first decryption method for the VOD session (e.g., page 11, lines 16-20, Fig. 3, item 244);

encrypting the first portions using the second encryption process at the second encryption device to produce encrypted first portions (e.g., page 13, lines 25-26, Fig. 2, item 132); and

assembling a stream of selectively encrypted content from the encrypted first portions and the second portions to produce a selectively encrypted stream of content that is individually encrypted for delivery during the VOD session (e.g., page 13, lines 20-21, Fig. 2, item 26).

Claim Group 2

Claim 11 is representative of Claim Group 2 below. According to certain embodiments as characterized by claim 11, a Video On Demand (VOD) method provides session based selective encryption (e.g., page 6, line 27 through page 7, line 5, Fig. 2, item 26):

processing content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted (e.g., page 13, lines 5-9, Fig. 2, items 108 and 112);

storing the first portions and storing the second portions (e.g., page 13, lines 10-11 and page 14, line 21 Fig. 3, item 208);

receiving a request for delivery of the content from a subscriber terminal to initiate a VOD session (e.g., page 13, line 13, Fig. 3, item 212);

determining if the subscriber terminal has decryption capabilities associated with a first decryption method or a second decryption method (e.g., page 13, lines 14-15, Fig. 2, item 104);

the request is from a subscriber terminal having decryption capabilities associated with the first decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the first decryption method to initiate a VOD session (e.g., page 13, lines 15-17, Fig. 3, item 216);

routing the first portions to a first encryption device that encrypts content for decryption under the first encryption method, to provide encryption of the first portions for the VOD session, and route the second portions around the first encryption device (e.g., page 14, lines 25-27, Fig. 3, item 222 and 226);

encrypting neither the first nor the second portions using a second encryption device that encrypts content for decryption under the second decryption method for the VOD session (e.g., page 11, lines 16-20, Fig. 2, item 104);

encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions (e.g., page 13, lines 19-20, Fig. 2, item 116);

assembling a stream of selectively encrypted content from the encrypted first portions and the second portions to produce a selectively encrypted stream of content that is individually encrypted for delivery during the VOD session (e.g., page 13, lines 20-21, Fig. 2, item 26);

if the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method, but instead the request is from a terminal having decryption capabilities associated with the second decryption method, then for each such request from a subscriber terminal having decryption capabilities the method instead initiates a VOD session associated with a second decryption method (e.g., page 13, lines 22-26, Fig. 2, items 112 and 132);

assembling a stream of content from the first portions and the second portions (e.g., page 13, lines 20–21, Fig. 2, item 26).

Claim Group 3

Claim 18 is representative of Claim Group 3 below. According to certain embodiments as characterized by claim 18, a Video On Demand (VOD) server arrangement that provides session based encryption, with means for receiving content from a selective encryption processor that processes content to be delivered in a VOD method by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted (e.g., page 13, lines 7–9, Fig. 2, items 108 and 112):

incorporating a router, first and second encryption devices, at least one computer readable storage device and a processor (e.g., page 13, lines 10–11, Fig. 1, item 22);

storing the first and second portions in the at least one computer readable storage device and receives a request for delivery of the VOD content as a VOD session, the request being from

a subscriber terminal having decryption capabilities associated with either a first decryption method or a second decryption method (e.g., page 13, lines 12–13, Fig. 3, item 212);

determining if the request is from a terminal having decryption capabilities associated with the first decryption method or the second decryption method (e.g., page 13, lines 14–15, Fig. 2, item 104);

if the request is from a terminal having decryption capabilities associated with the first decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the first decryption method to initiate a VOD session in which the processor instructs the router to route the first portions to the first encryption device and not the second encryption device, and routes the second portions around the first encryption device and around the second encryption device to allow a first encryption device to encrypt the first portions using a first encryption process (e.g., page 13, lines 15–19, Fig. 3, items 216 and 222);

If, however, the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method, then routing the first portions to the second encryption device that encrypts content for decryption under the second encryption method, to provide encryption of the first portions for the VOD session (e.g., page 13, lines 22–23, Fig. 2, items 112 and 132);

routing the second portions around the second encryption device and encrypting neither the first nor the second portions using the first encryption device that encrypts content for decryption under the first decryption method for the VOD session (e.g., page 13, lines 24 -25, Fig. 3, item 244);

encrypting the first portions using the second encryption process at the second encryption device to produce encrypted first portions, and assembling a stream of selectively encrypted content from the encrypted first portions and the second portions (e.g., page 13, lines 20–26, Fig. 2, items 26, 128 and 132);

if the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method, but instead the request is from a terminal having decryption capabilities associated with the second decryption method, then for each such request from a

subscriber terminal having decryption capabilities associated with the second decryption method to initiate a VOD session (e.g., page 14, lines 11 -12, Fig. 2, items 26 and 132);

instructing the first router to route the stream to a second encryption device and the second encryption device encrypts the first portions using a second encryption process to produce a selectively encrypted stream (e.g., page 14, lines 13–16, Fig. 2, item 46).

Claim Group 4

Claim 19 is representative of Claim Group 4 below. According to certain embodiments as characterized by claim 19, a server arrangement having a request from a terminal having decryption capabilities associated with the second decryption method, for each such request from a subscriber terminal having decryption capabilities associated with the second decryption method to initiate a VOD session (Page 13, lines 22-23, Fig. 2, items 26 and 132):

the means for assembling assembles a stream of content from the first portion and the second portion (Page 13, lines 23-24, Fig. 2, item 26);

the processor instructs the first router to route the stream to a second encryption device (Page 13, lines 24-25, Fig. 2, item 22);

and wherein the second encryption device encrypts the first portions using a second encryption process to produce a selectively encrypted stream (Page 13, lines 24-25, Fig. 2, item 46).

Claim Group 5

Claim 24 is representative of Claim Group 5 below. According to certain embodiments as characterized by claim 24, a VOD method that provides session based encryption by receiving a request for delivery of content from a subscriber terminal (Page 17, lines 18-19, Fig. 3, item 212):

retrieving the content from a storage medium (Page 17, lines 19-20, Fig. 2, item 18);

processing the retrieved content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted (Page 17, lines 20-22, Fig. 3, item 222);

determining if the request is from a subscriber terminal having decryption capabilities associated with a first decryption method or a second decryption method (Page 17, lines 22-24, Fig. 2, item 30);

for each request from a subscriber terminal having decryption capabilities associated with the first decryption method to initiate a VOD session routing the first portions to a first encryption device (Page 17, lines 24-26, Fig. 2, item 26);

routing the second portions around the first encryption device (Page 17, lines 26-27, Fig. 2, item 112);

encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions (Page 17, lines 27-28, Fig. 2, item 116);

and assembling a stream of selectively encrypted content from the encrypted first portions and the second portions to produce a selectively encrypted stream of content that is individually encrypted for delivery during the VOD session (Page 17, lines 28-29, Fig. 2, item 26).

Claim Group 6

Claim 30 is representative of Claim Group 6 below. According to certain embodiments as characterized by claim 30, the VOD method for each request from a subscriber terminal having decryption capabilities associated with the second decryption method to initiate a VOD session (Page 15, lines 1-2, Fig. 2, item 30):

assembling a stream of content from the first portion and the second portion (Page 15, lines 2-3, Fig. 2, item 26);

routing the stream to a second encryption device (Page 15, lines 3-4, Fig. 2, item 112);

and encrypting the first portions using a second encryption process at the second encryption device to produce a selectively encrypted stream of content that is individually encrypted for delivery during the VOD session (Page 15, lines 4-6, Fig. 2, item 132).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-6 and 8-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over So (US Patent Application Publication No. 2002/0083438, published 6/27/2002) in view of Colligan (US Patent No. 6,415,031, filed March 20, 2000).

GROUPING OF CLAIMS

Group 1: Claims 1–10 stand or fall together.

Group 2: Claims 11–17 stand or fall together.

Group 3: Claims 18 and 20-22 stand or fall together.

Group 4: Claims 19 and 23 stand or fall together.

Group 5: Claims 24–29 stand or fall together.

Group 6: Claims 30–33 stand or fall together.

ARGUMENTS

The arguments herein present the errors of the Examiner in the analysis of the claims as filed against the cited prior art. It is noted that at various points in the arguments, the explicit claim language may be paraphrased for ease of understanding; however, this is done for convenience and brevity and without intent of imposing limitations on the claims.

It is the initial burden of the Examiner to establish *prima facie* unpatentability ["The examiner bears the initial burden...of presenting a *prima facie* case of unpatentability." *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992).]. In a rejection for obviousness, this is done by use of the factual inquiries of *Graham v. Deere*, 383 U.S. 1, 148 USPQ 459 (1966). It is respectfully submitted that the Examiner has erred in failing to meet this burden. In order to properly hold a claim as obvious the Supreme Court in *Graham v. Deere*, 383 U.S. 1, 148 USPQ 459 (1966) has set forth four factual inquires that must be met:

1. Determining the scope and contents of the prior art;
2. Ascertaining the differences between the prior art and the claims in issue;
3. Resolving the level of ordinary skill in the pertinent art; and

4. Evaluating evidence of secondary considerations.

Appellants comments below show that the Examiner erred at least in not properly meeting inquiry 1, determining the scope and contents of the prior art, and inquiry 2, ascertaining the differences between the prior art and the claims in issue, (as numbered above – hereinafter "inquiry 1" and "inquiry 2") of the factual inquires of *Graham v. Deere* and has thus failed to show a *prima facie* case for rejection of the claims as obvious under 35 U.S.C. §103.

Regarding Claim Group 1:

Claim 1 is representative of this group.

1) The Examiner has failed to identify all elements of the claims in the cited art arranged in the manner required by the claims.

Referring to claim 1, this claim calls out a process for "session based selective encryption", meaning that encryption occurs upon request for content by a subscriber (a session). This form of encryption naturally flows from the language of the claims as discussed below and has also been referred to in the various arguments of record as "real time encryption" (an essentially equivalent term used by So), since the encryption happens on demand.

It is respectfully submitted that the Examiner erred in stating that the So reference discloses session based encryption as claimed, looking to paragraphs 45 and 106 for this specific teaching. Paragraph 45 of the So reference specifically states, in line 4, "granting access to *pre-encrypted* content" (emphasis added). Neither paragraphs 45 nor 106 disclose or teach "processing content by selecting first portions of the content for encryption under a selective encryption system" as recited in claim 1.

Additionally, Claim 1 goes on to call for "processing content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted; storing the first portions;" and "storing second portions." The Final Office Action alleges that So discloses these claim features in paragraph [0106]. However, So only discloses a scrambling control field that identifies whether or not packets are

encrypted . There is no teaching of either selection of particular packets or storing first and second portions as claimed. Hence, these claim features have not been properly identified in So.

2) So fails to teach selective multiple encryption as claimed and fails to teach that decisions are made based upon the capabilities of the subscriber terminal

Claim 1 goes on to call for "receiving a request for delivery of the content from a subscriber terminal to initiate a VOD session;" and "determining if the subscriber terminal has decryption capabilities associated with a first decryption method or a second decryption method".

The Final Office Action alleges that So discloses these claim features in paragraphs [0058] and [0063]. However, paragraph [0063] of So, in fact only discloses a VOD enablement system based on payment or other parameters. The Office Action alleges that the CAS system "determines cryptographic parameters" and that the "EMM signals match the capabilities of terminals with the encryption protocol, and therefore the capabilities of subscriber terminals are determined and considered". Appellant finds no such teaching. So actually only says "the CAS 110 permits access to pre-encrypted content by subscriber terminals by provisioning the subscriber terminals with EMMs, and generating ECMs for non-VOD services."

However, even if this is the case nothing about this suggests "determining if the subscriber terminal has decryption capabilities associated with a first decryption method or a second decryption method" as required by the claims. Nowhere does this reference teach or suggest distinguishing between first and second decryption methods based upon a subscriber terminal's capabilities. So's system is simply not disclosed to have the capabilities of distinguishing between subscriber terminals ability to decrypt either first or second decryption methods as claimed.

On the contrary, So teaches performing one type of encryption on all content, regardless of session, and performing this encryption in an offline, non-real-time manner. There is no teaching or suggestion of multiple selective encryption as claimed.

3) So does not teach assembly of content for multiple different types of encryption devices

Claim 1 calls for "if the request is from a subscriber terminal having decryption capabilities associated with the first decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the first decryption method to initiate a VOD session:

routing the first portions to a first encryption device that encrypts content for decryption under the first encryption method, to provide encryption of the first portions for the VOD session;

routing the second portions around the first encryption device;

encrypting neither the first nor the second portions using a second encryption device that encrypts content for decryption under the second decryption method for the VOD session;

encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions".

The Final Office Action alleges that So discloses these claim features in paragraph [0051]. The Office Action states that "So encrypts the content according to the capabilities of the requesting terminal, and won't perform any encryption that cannot be decrypted by the receiving terminal". Appellant respectfully disagrees. There is no teaching or suggestion in So of selection between two encryption methods based upon the capabilities of the requesting terminal. In fact, Appellant finds no suggestion that more than one type of encryption is contemplated by So in any given system. (Moreover it is noted there is no teaching in So to support the allegation that 'So won't encrypt something that can't be decrypted by the receiving terminal'. The Examiner has erred in making this assertion which is not supported by So. In fact, since VOD signals are broadcast to multiple terminals and are thus receivable by receiver terminals not associated with the requesting terminal, So will in fact encrypt content that cannot be decrypted by a receiving terminal.)

So simply does not provide any mechanism for selecting between two encryption techniques and does not route a stored portion to a first encryption device for encryption and

route a second stored portion around the first and second encryption device to prevent encryption under the first or second encryption method as claimed. Moreover, So does not teach doing so on the basis of the decryption capabilities of a subscriber terminal.

The Office Action further asserts that paragraph [0051] discloses "the CPS encrypts the content according to CAS specifications", however, nowhere is there any teaching or suggestion that those specifications involve selection of an encryption method based upon decryption capabilities of the subscriber terminal. So, in fact, uses the CPS to instruct the OLES to carry out the pre-encryption (per paragraph [0053]) without the precondition of determination of the decryption capabilities of the subscriber terminal. Recall that the claim is directed to a "session based" encryption method that does not use pre-encryption.

The Examiner also erred in asserting that the So reference teaches content delivery to one or more cable systems, looking to paragraphs 19 and 160 and Figure 5 for support of this erroneous assertion. Paragraph 19 discloses the delivery of "content from a head end to subscriber terminals within one or more cable systems". Paragraph 160 refers the reader to Figure 5, which shows a diagram of the delivery of content from a provider, through a cable head-end box, and then to multiple subscribers. However, there is no teaching or suggestion that the multiple cable systems in So utilize different encryption and decryption methods. Appellant submits that in fact the multiple cable systems referenced in So to which content is delivered are evidently of the same type, and use the same encryption type. There is no teaching or suggestion otherwise. Hence, So's teachings are actually directed to content delivery to multiple subscribers from the same service provider, not to different cable systems, which would have different content processing functions with different encryption. Thus, while So may show content delivery to two cable systems, there is no teaching or suggestion that these systems use different encryption.

Claim 1 then calls for "if the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method:

> routing the first portions to a second encryption device that encrypts content for decryption under the second encryption method, to provide encryption of the first portions for the VOD session;

routing the second portions around the second encryption device;

encrypting neither the first nor the second portions using the first encryption device that encrypts content for decryption under the first decryption method for the VOD session;

encrypting the first portions using the second encryption process at the second encryption device to produce encrypted first portions".

The Final Office Action alleges that So teaches these features in paragraphs [0051], [0063] and [0161]. Appellant has examined these paragraphs and respectfully disagrees and submits that the Examiner has erred in this assertion. So in fact discloses the serial use of a plurality of encryption keys but using only one at a time for his pre-encrypted content. Upon examination, it is clear that So has no teachings applicable to selection of a routing of content based upon a decryption capability of a subscribing station in the manner claimed above.

Paragraph [0051] of So describes operation of the CPS. Paragraph [0063] of So describes operation of the CAS. Paragraph [0161] shows multiple cable systems that share a single encryption system (within the CPS). There is nothing that suggests that the multiple cable systems utilize differing encryption methods. In fact, by sharing a single CPS containing the OLES one must assume, if anything, that in fact the same encryption is used by the multiple cable systems.

4) So teaches against real-time encryption

With regard to the So reference, the Examiner erred in characterizing the So reference as teaching "real time encryption" simply because the So reference mentions "real time encryption". The So reference, in paragraph [0015] discloses "*disadvantageously*, for VOD, real-time encryption poses much greater cost and space issues" (emphasis added), and goes on to disclose, in paragraph [0017] that his invention is "Unlike related art systems that employ real time encryption" and he discloses that his system "allows content to be encrypted once, at a centralized facility" and that "there is no need to reprocess the pre-encrypted contents". These points are presented repeatedly as advantages of the system disclosed in So of encrypting content

once, prior to delivery of the content, and not processing the content again such that the cost and space issues of real-time encryption may be overcome by the system of So. The Examiner presents the argument that "identifying the disadvantages of real time encryption is not equivalent of teaching against real time encryption" in the office action. However, the Examiner erred in not considering that So not only discloses that real time encryption has disadvantages, but that the system disclosed in So has advantages over and is inconsistent with real time encryption in encrypting data only once and delivering the pre-encrypted data as needed. The So reference discloses real-time encryption as a disadvantageous process for encrypting content. So also discloses that off-line, non-real-time encryption of content is a superior way to accomplish encryption of content. In the So reference as a whole, this combination of disclosing the disadvantages of real-time encryption and disclosing an advantage of another system over real-time encryption clearly does in fact provide a teaching against real-time encryption of content.

The claim also calls for "assembling a stream of selectively encrypted content from the encrypted first portions and the second portions to produce a selectively encrypted stream of content that is individually encrypted for delivery during the VOD session."

The Final Office Action alleges that So teaches these features in paragraph [0106]. However, paragraph [0106] serves only to teach how scrambling control bits can be used to identify that a particular packet has been encrypted. There is no teaching relevant to the process that leads to the creation of the claim elements of the "first portion" and the "second portion" in accord with the claimed process.

5) So cannot be logically combined with real time encryption on demand

The Office Action uses the Colligan reference for teaching of the encryption after each request. However, this is inherently contradictory to So's teachings.

The Examiner erred in stating that "there is nothing in So that prevents combining it with a reference that performs real-time encryption". It is submitted that it is the Examiner's obligation to establish that one of ordinary skill in the art would be motivated to make such a combination – there being nothing to prevent the combination is both inaccurate and inadequate to establish *prima facie* obviousness. It is Appellant's position that the combination of teaching

disadvantages of a real-time encryption system, as disclosed in paragraph 15, and the teachings in paragraph 17 of "*unlike* (emphasis added) related art systems that employ real-time encryption, the embodiments of the present system encrypt content off-line" and there being "no need to reprocess the pre-encrypted content" do indeed prevent the combination of So with other references to teach the performance of real-time encryption as this teaching shows that there could be no desirability of combination. Moreover, there is no enabling teaching of record and no articulated reasoning presented as to how one would accomplish a combination of real-time encryption with the pre-encryption taught by So.

In view of the above, it is clear that So does not in fact contain the teachings alleged by the Office Action, and hence, the Examiner has failed to establish *prima facie* obviousness since the Graham inquiries require 1) that the scope and content of the prior art be determined and that 2) the differences be resolved between the prior art and the claims. In view of these failures, the combination of So and Colligan fails to meet the claim features and *prima facie* obviousness has not been established. Reconsideration and reversal of the rejections to claim group 1 are respectfully requested.

The Examiner also erred in his assertion that "A person skilled in art would be motivated to combine so that they could service both the legacy system using real-time encryption and systems that use pre-encryption". The Final Office Action asserts that the motivation to combine "lies in the fact that VOD subscribers have a variety of set top system and it is desirable to service all of them". This assertion is without basis. In fact, subscribers and indeed cable systems are essentially locked into one system or another based upon heretofore incompatible proprietary encryption systems for VOD. There is no variety of set top systems that use differing decryption systems for VOD in a single cable system, for example, except for those proposed by Appellants and their colleagues. There is need for an ability to have a variety of set top systems in a single cable system, but this problem remained unresolved prior to Applicant's inventions related to solutions to this problem. Until applicant's inventions utilizing multiple selective encryption within a VOD system, this need was unfulfilled due to the high cost of large numbers of encrypters and large bandwidth requirements (as is essentially acknowledged in So in connection with his description of the disadvantages of real time encryption). Hence, the Examiner has

erred in using the Applicant's own teachings in hindsight analysis, and has failed to consider the secondary considerations of the need for such a system as that of Applicant.

6) The combination of So and Colligan is not enabled and there is no articulated reasoning for making the proposed combination

The Examiner admits that the So reference does not disclose encrypting the content of a message after each request and looks to the Colligan reference to remedy this lack. However, while Colligan may describe a system in which the content is encrypted on request, the Examiner has failed to reconcile how encryption on demand is combined with pre-encryption of the content which is purported to be superior to and apparently a replacement for encryption on demand (assuming the benefits espoused by So are to be realized). In view of the inherent contradiction in the approaches of So and Colligan, more than a passing reference to Colligan disclosing that content is encrypted after each request is required. Any reasoning for such a combination would appear to be inherently contradictory, and would require a showing that the resulting structure would be enabled by the art. Appellant finds no viable reasoning in the Final Office Action.

7) Modification of So destroys its intended function

It is further submitted that So relates to a system for pre-encryption of content and favors such pre-encryption over purportedly disadvantageous real-time encryption. The objectives of So would be defeated by a modification of So that incorporates any real time encryption (which he fervently advocates against). Any modification that would introduce real time encryption would be an improper modification of So since it would re-introduce all of the disadvantages that So preaches so strongly against in connection therewith. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984) stands for the proposition that "if proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification". Modification of So to incorporate real-time encryption would make So unsatisfactory for its intended purpose by reintroduction of all the disadvantages So seeks to be free of.

While the rigid application of the so-called TSM test has been recently curbed (but only to the extent that it is applied as a rigid rule) by the Supreme Court, the Court did not strike down and in fact affirmed the principle that the Office bears the burden of establishing articulated reasoning as to why one of ordinary skill in the art would make a proposed modification or combination. The principle of *Gordon* is believed to remain sound. In the absence of an articulated reasoning (as required by *In re Kahn*, 441 F.3d 977, 988 (C.A.Fed.2006) ("Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness") and explicitly endorsed by the Supreme Court in *KSR Int'l Co. v. Teleflex Inc.*, 82 USPQ2d 1385 U.S. Supreme Court (2007)) as to why one of ordinary skill in the art would disregard the disadvantages and explicit teaching against real-time encryption as espoused by So (e.g., at paragraphs [0015] and [0018]) and then modify So to use the very technology he teaches against, it is believed clear that one of ordinary skill in the art would not find the combination obvious and it is believed that the combination and associated rejections are improper.

8) Conclusion.

Appellant respectfully submits that the Examiner has failed to establish *prima facie* obviousness with regard to the claims in Group 1. The Examiner erred in not properly determining the scope and contents of the prior art as required by inquiry 1 of the *Graham v. Deere* inquiries, maintaining that the So reference teaches real-time encryption of content when the reference as a whole actually teaches against real-time encryption of content and fails to disclose features that are called for by the claims. The Examiner also erred in not properly ascertaining the differences between the prior art and the claims in issue as required by inquiry 2 of the *Graham v. Deere* inquiries.

Hence, as shown above, the Examiner has failed to identify all elements of the claims in the cited art arranged in the manner required by the claims. As shown above, the So reference fails to provide teaching of the claim features asserted to be taught, such as multiple encryption

and session-based encryption of content, as are clearly recited in the claims of Group 1. The So reference is directed to the pre-encryption of content and the storage thereof for later delivery.

So fails to teach selective multiple encryption as claimed and fails to teach that decisions are made based upon the capabilities of the subscriber terminal. Nowhere does the So reference teach or suggest distinguishing between first and second decryption methods based upon a subscriber terminal's capabilities.

So does not teach assembly of content for multiple different types of encryption. There is no teaching in So to support the allegation that "So encrypts content according to the capabilities of the receiving terminal" to the extent this means specifying an encryption method". The Examiner has erred in making this assertion which is not supported by So. In fact, since VOD signals are broadcast to multiple terminals and are thus receivable by receiver terminals not associated with the requesting terminal, So will in fact encrypt content that cannot be decrypted by a receiving terminal.

So in fact teaches against real-time encryption. The So reference discloses real-time encryption as a disadvantageous process for encrypting content. So also discloses that off-line, non-real-time encryption of content is a superior way to accomplish encryption of content. In the So reference as a whole, this combination of disclosing the disadvantages of real-time encryption and disclosing an advantage of another system over real-time encryption clearly does in fact provide a teaching against real-time encryption of content that has not been properly considered.

So cannot be logically combined with real time encryption on demand. It is Appellant's position that the combination of teaching disadvantages of a real-time encryption system, as disclosed in paragraph 15, and the teachings in paragraph 17 of "*unlike* (emphasis added) related art systems that employ real-time encryption, the embodiments of the present system encrypt content off-line" and there being "no need to reprocess the pre-encrypted content" do indeed prevent the combination of So with other references to teach the performance of real-time encryption as this teaching shows that there could be no desirability of combination. Moreover, there is no enabling teaching of record and no articulated reasoning presented as to how one would accomplish a combination of real-time encryption with the pre-encryption taught by So.

The combination of So and Colligan is not enabled and there is no articulated reasoning for making the proposed combination. Modification of So destroys its intended function. In the absence of an articulated reasoning as to why one of ordinary skill in the art would disregard the disadvantages and explicit teaching against real-time encryption as espoused by So (e.g., at paragraphs [0015] and [0018]) and then modify So to use the very technology he teaches against, it is believed clear that one of ordinary skill in the art would not find the combination obvious and it is believed that the combination and associated rejections are improper.

Therefore, Appellant respectfully submits that the claims of Group 1 are allowable for at least these reasons. Reversal of the rejections to Claim Group 1 by the Board is respectfully requested.

Regarding Claim Group 2:

Claim 11 is representative of this group. The above remarks are equally applicable to this group.

1) Additional features of the claim are not met by the cited art

In addition to elements presented for claim 1, this claim recites

"if the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method, but instead the request is from a terminal having decryption capabilities associated with the second decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the second decryption method to initiate a VOD session:

Assembling a stream of content from the first portion and the second portion, routing the stream to the second encryption device, and encrypting the first portions using the second encryption device to produce an encrypted stream of content that is individually encrypted for delivery during the VOD session."

It is respectfully submitted that the Examiner erred in asserting that the So reference teaches these claim features. Appellant simply finds no such teaching in So and no guidance in the Office Action as to where such teaching would be found.

2) There is only one encryption device for each content package in So

The Final Office Action errs in the assertion that there is more than one encryption device providing encryption of content disclosed in the So reference. The Final Office Action looks to paragraph 51 for a teaching of "Assembling a stream of content from the first portion and the second portion, routing the stream to the second encryption device, and encrypting the first portions using the second encryption device."

Paragraph 51 of the So reference discloses that the Content Preparation System (CPS) is a sufficient way to prepare content according to the requirements of the CAS. In paragraph 53, the So reference discloses that the requirements of the CAS are met through the use of an OLES (offline encryption) device. The OLES may provide for a plurality of encryption devices, but once an encryption device is selected for use the entire content package is pre-encrypted, offline, using that one encryption device and the pre-encrypted content is then saved in memory storage until it is needed. Nowhere does this reference teach or disclose "routing the stream to the second encryption device, and encrypting the first portions using the second encryption device" as required by the claims. Moreover, there is no discussion of routing a portion of content around an encryption device.

3) There is no teaching of session based encryption of content based upon decryption capabilities

Claim 11 further recites "encrypting the first portions using the second encryption device to produce an encrypted stream of content that is individually encrypted for delivery during the VOD session." The So reference actually teaches a non-real-time encryption device in paragraph 51, which device cannot perform encryption on a session basis as sessions are real-time constructs and the So reference in paragraphs 51 and 53 disclose a non-real-time, offline encryption device and method.

The So reference does not provide for the encryption of first and second portions of a single content stream being encrypted using different encryption devices as there is only one device, the OLES, which encrypts content offline apparently using one encryption device per content package. Moreover, there is no decryption based on the decryption capabilities of the

subscriber terminal disclosed or suggested. Therefore, the Examiner has erred in asserting that these claim elements are met by the So reference.

4) The combination of So and Colligan is not enabled and there is no articulated reasoning for making the proposed combination

The Examiner admits that the So reference does not disclose encrypting the content of a message after each request and looks to the Colligan reference to remedy this lack. However, while Colligan may describe a system in which the content is encrypted on request, the Examiner has failed to reconcile how encryption on demand is combined with pre-encryption of the content which is purported to be superior to and apparently a replacement for encryption on demand (assuming the benefits espoused by So are to be realized). In view of the inherent contradiction in the approaches of So and Colligan, more than a passing reference to Colligan disclosing that content is encrypted after each request is required. Any reasoning for such a combination would appear to be inherently contradictory, and moreover, would require a showing that the resulting structure would be enabled by the art and obvious to one of ordinary skill in the art.

5) Conclusion.

Appellant respectfully submits that the Examiner has failed to establish *prima facie* obviousness with regard to the claims in Group 2. All reasoning presented in connection with Claim Group 1 is equally applicable and in addition, the Examiner erred in not properly determining the scope and contents of the prior art as required by inquiry 1 of the *Graham v. Deere* inquiries, maintaining that the So reference teaches session-based, real-time encryption of content when the reference as a whole actually teaches against session-based, real-time encryption of content and fails to disclose features that are called for by the claims. The Examiner also erred in not properly ascertaining the differences between the prior art and the claims in issue as required by inquiry 2 of the *Graham v. Deere* inquiries.

As shown above, Additional features of the claim are not met by the cited art. Appellant finds no teaching in So for the additional features of this claim group.

There is only one means for encryption for each content package. There is no disclosure or teaching in So that provides for the encryption of a portion of the content using a first encryption device and another portion of the same content to be encrypted using a second encryption device with each device using a different encryption method. The OLES disclosed in So may provide for a plurality of encryption means, but once an encryption device is selected for use the entire content package is pre-encrypted, offline, using that one encryption device and method and the pre-encrypted content is then saved in memory storage until it is needed. Nowhere does this reference teach or disclose 'routing the stream to the second encryption device, and encrypting the first portions using the second encryption device' as required by the claims.

There is no teaching of session based selective encryption of content. The So reference discloses a non-real-time encryption device in paragraph 51, which device cannot perform encryption on a session basis as sessions are real-time constructs and the So reference in paragraphs 51 and 53 disclose a non-real-time, offline encryption device and method.

The combination of So and Colligan is not enabled and there is no articulated reasoning for making the proposed combination. In view of the inherent contradiction in the approaches of So and Colligan, more than a passing reference to Colligan disclosing that content is encrypted after each request is required. Any articulated reasoning would appear to be inherently contradictory, and would require a showing that the resulting structure would be enabled by the art.

Appellant respectfully submits that the claims of Group 2 are allowable for at least these reasons. Reversal of the rejections to Claim Group 2 by the Board is respectfully requested.

Regarding Claim Group 3:

Claim 18 is representative of this group. The above remarks in connection with Claim Group 1 are equally applicable to this group.

1) No articulated reasoning has been provided with regard to the cited prior art

It is respectfully submitted that the Examiner has erred in asserting, in section 7.10 of the Final Office Action, that claims 18–33 are "disclosed by So". Therefore, the Appellant is directed by Examiner's statement of section 7.10 to look solely to the So reference for teachings with regard to the claims of claim group 3, and thus claim 18.

Additionally, the Examiner has erred in not presenting direction as to how each claim is rejected under this reference other than by the vague statement "as described by responses to claims 1 to 17" in section 7.10 of the office action. The Examiner has not supplied an "articulated reasoning" for the rejection of the claims in claim Group 3 per *In re Kahn*, supra.

2) Additional claim elements are not disclosed or taught by So

In addition to elements presented for claim 1, this claim recites

"receives a request for delivery of the VOD content as a VOD session, the request being from a subscriber terminal having decryption capabilities associated with either a first decryption method or a second decryption method" and "the processor instructs the router to route the first portions to the first encryption device and not the second encryption device."

It is unclear to the Appellant what teaching the Final Office Action looks to for a teaching of these claim elements. The Examiner has erred in not providing a disclosure for these claim elements within the So reference or an articulated reasoning as to why any such disclosure teaches the recited claim elements. The Appellant asserts that there is no disclosure or teaching within the So reference for the claim elements recited above and, as such, there is no basis under the *Graham v. Deere* inquiry 1, "ascertaining the differences between the prior art and the claims in issue", for a rejection under 35 U.S.C. 103(a).

3) Conclusion

Appellant respectfully submits that the Examiner has failed to establish *prima facie* obviousness with regard to the claims in Group 3. Each of the reasons argued in connection with Claim Group 1 are equally applicable. The Examiner erred in not properly determining the scope and contents of the prior art as required by inquiry 1 of the *Graham v. Deere* inquiries as

shown above. The Examiner also erred in not properly ascertaining the differences between the prior art and the claims in issue as required by inquiry 2 of the *Graham v. Deere* inquiries.

The Examiner has not supplied an "articulated reasoning" for the rejection of the claims in claim Group 3 per *In re Kahn*, supra.

Additional claim elements are not disclosed or taught by So. The Examiner has not provided a disclosure for additional claim elements within the So reference or an articulated reasoning as to why any such disclosure teaches the additional claim elements. The Appellant asserts that there is no disclosure or teaching within the So reference for the claim elements recited in Claim Group 3.

Additionally, the So reference fails to provide any teaching of the claim features such as "multiple encryption by a plurality of devices within one content package" and "session-based encryption of content", as are clearly recited in the claims of Group 3.

Appellant respectfully submits that the claims of Group 3 are allowable for at least these reasons. Reversal of the rejections to Claim Group 3 by the Board is respectfully requested.

Regarding Claim Group 4:

Claim 19 is representative of this group.

1) No articulated reasoning with regard to the cited prior art

It is respectfully submitted that the Examiner has erred in asserting, in section 7.10 of the Final Office Action, that claims 18–33 are "disclosed by So". Therefore, the Appellant is directed by Examiner's statement of section 7.10 to look solely to the So reference for teachings with regard to the claims of claim group 3, and thus claim 19.

Additionally, the Examiner has erred in not presenting direction as to how each claim is rejected under this reference other than by the vague statement "as described by responses to claims 1 to 17" in section 7.10 of the office action. The Examiner has not supplied an "articulated reasoning" for the rejection of the claims in claim Group 4 per *In re Kahn*, supra.

2) Claim elements not disclosed or taught by So

Claim 19 recites at least "if the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method, but instead the request is from a terminal having decryption capabilities associated with the second decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the second decryption method to initiate a VOD session... wherein the second encryption device encrypts the first portions using a second encryption process to produce a selectively encrypted stream." Appellant is uncertain as to the disclosure or articulated reasoning for any such disclosure within the So reference that the Final Office Action looks to for support in the rejection of these claims. Even if the Examiner has provided a disclosure and articulated reasoning, the So reference does not provide a disclosure or teaching for the recited claim elements. For example, the So reference discloses in paragraphs 17 and 53 that "content is encrypted once" and "CPS includes an OLES (offline encryption) device for performing" the offline encryption. Clearly, the So reference discloses performing encryption, through the use of one device, the OLES. The So reference teaches against real-time encryption, as presented above, and, therefore, could not produce a selectively encrypted stream of content as streaming data is a real-time activity.

Additionally, claim 19 calls for a processor instructing the first router to route the stream and a second encryption device. The Examiner has erred in not providing guidance as to where such claim features can be found in So.

3) Conclusion

Appellant respectfully submits that the Examiner has failed in presenting a prima facie case of obviousness with regard to the claims in Group 4. All arguments related to Claim Groups 1 and 3 are equally applicable. The Examiner erred in not properly determining the scope and contents of the prior art as required by inquiry 1, maintaining that the So reference teaches real-time encryption of content when the reference as a whole actually teaches against real-time encryption of content. The Examiner also erred in not properly ascertaining the differences between the prior art and the claims in issue as required by inquiry 2, as shown

above, the So reference teaches against real-time encryption of content and this feature is clearly recited in the claims of Group 4.

No articulated reasoning with regard to the cited prior art has been provided, so the Examiner has erred in not presenting direction as to how each claim is rejected under this reference. Claim elements are present that are not disclosed or taught by So. The Examiner has not provided a disclosure for additional claim elements as recited above within the So reference or an articulated reasoning as to why any such disclosure teaches the additional claim elements. The Appellant asserts that there is no disclosure or teaching within the So reference for the claim elements recited in Claim Group 4.

Appellant respectfully submits that the claims of Group 4 are allowable for at least these reasons. Reversal of the rejections to Claim Group 2 by the Board is respectfully requested.

Regarding Claim Group 5:

Claim 24 is representative of this group. The above remarks regarding Claim Groups 1 and 2 are equally applicable to this group.

1) No articulated reasoning with regard to the cited prior art

It is respectfully submitted that the Examiner has erred in asserting, in section 7.10 of the Final Office Action, that claims 18 – 33 are "disclosed by So". Therefore, the Appellant is directed by Examiner's statement of section 7.10 to look solely to the So reference for teachings with regard to the claims of claim group 5, and thus claim 24.

Additionally, the Examiner has erred in not presenting direction as to how each claim is rejected under this reference other than by the vague statement "as described by responses to claims 1 to 17" in section 7.10 of the office action. The Examiner has not supplied an "articulated reasoning" for the rejection of the claims in claim Group 3 per *In re Kahn*, supra.

2) Additional claim elements not disclosed or taught by So

In addition to arguments presented for Claim Groups 1 and 2 above, this claim recites

"processing the retrieved content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted."

Appellant is uncertain as to the disclosure or articulated reasoning for any disclosure within the So reference that the Final Office Action looks to for support in the rejection of these claim elements. Even if the Examiner has provided a disclosure and articulated reasoning, the So reference does not provide a disclosure or teaching for the recited claim elements. For example, Paragraph 51 discloses a Content Preparation System (CPS) that "encodes content in a format (e.g., MPEG2) suitable for storage on video servers and for distribution to the subscriber terminals". This is not the same as "processing the retrieved content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted." The CPS is simply the mechanism used to place content into a format that is acceptable to players that will receive the content at the subscriber locations. Paragraph 53 of the So reference describes the CPS as including an Offline Encryption (OLES) device for performing content preparation. In paragraph 53 the OLES "uses one or more non-real-time, or offline, encryption devices to encrypt content". Thus, the CPS is not a session based utility at all, but rather an offline service that encrypts content one time and stores it away. There is no teaching that is directed to a real-time, session based system that provides for encryption using more than one type of encryption for various portions of content to be encrypted. On the contrary, So teaches performing one type of encryption on all content, regardless of session, and performing this encryption in an offline, non-real-time manner. If an encryption method is selected according to the capabilities of the subscriber terminal, there is no teaching as to how this is accomplished for multiple types of subscriber terminals in the cited references.

Additionally, claim 24 calls for determining if a request is from a subscriber terminal having decryption capabilities associated with a first or a second encryption method and routing portions of content accordingly. The Examiner has erred in not providing guidance as to where such claim features can be found in So.

3) Conclusion

Appellant respectfully submits that the Examiner has failed in presenting a prima facie case of obviousness with regard to the claims in Group 5. The arguments relating to Claim Groups 1 and 2 are applicable to this group. The Examiner erred in not properly determining the scope and contents of the prior art as required by inquiry 1, maintaining that the So reference teaches real-time encryption of content when the reference as a whole actually teaches against real-time encryption of content. The Examiner also erred in not properly ascertaining the differences between the prior art and the claims in issue as required by inquiry 2, as shown above, the So reference teaches against real-time encryption of content and this feature is clearly recited in the claims of Group 5.

No articulated reasoning has been provided with regard to the cited prior art. The Examiner has not supplied an "articulated reasoning" for the rejection of the claims in claim Group 3.

The Examiner has not provided a disclosure for additional claim elements as recited above within the So reference or an articulated reasoning as to why any such disclosure teaches the additional claim elements. The Appellant asserts that there is no disclosure or teaching within the So reference for the claim elements recited in Claim Group 5.

Appellant respectfully submits that the claims of Group 5 are allowable for at least these reasons. Reversal of the rejections to Claim Group 2 by the Board is respectfully requested.

Regarding Claim Group 6:

Claim 30 is representative of this group. The above remarks are equally applicable to this group.

1) No articulated reasoning with regard to the cited prior art

It is respectfully submitted that the Examiner has erred in asserting, in section 7.10 of the Final Office Action, that claims 18 – 33 are "disclosed by So". Therefore, the Appellant is again apparently directed by Examiner's statement of section 7.10 to look solely to the So reference for teachings with regard to the claims of claim group 6, and thus claim 30.

Additionally, the Examiner has erred in not presenting direction as to how each claim is rejected under this reference other than by the vague statement "as described by responses to claims 1 to 17" in section 7.10 of the office action. The Examiner has not supplied an "articulated reasoning" for the rejection of the claims in claim Group 3 per *In re Kahn*, supra.

2) Additional claim elements not disclosed or taught by So

In addition to elements presented for claim 1 above, this claim recites

"encrypting the first portions using a second encryption process at the second encryption device to produce a selectively encrypted stream of content that is individually encrypted for delivery during the VOD session."

Appellant is uncertain as to the disclosure or articulated reasoning for any disclosure within the So reference that the Final Office Action looks to for support in the rejection of these claim elements. Even if the Examiner has provided a disclosure and articulated reasoning, the So reference does not provide a disclosure or teaching for the recited claim elements. For example, the So reference discloses in paragraphs 17 and 53 that "content is encrypted once" and "CPS includes an OLES (offline encryption) device for performing" the offline encryption. Clearly, the So reference is discloses performing encryption, through the use of one device, the OLES. The So reference teaches against real-time encryption, as presented above, and, therefore, could not produce a selectively encrypted stream of content as streaming data is a real-time activity. Additionally, the So reference provides no teaching or disclosure that a selectively encrypted stream of content is individually encrypted for delivery during a VOD session according to the capabilities of the subscriber station requesting content. The disclosure in So, paragraph 17, provides only for a one time encryption of content. Paragraph 53 of So discloses that this one time encryption occurs off-line, in a non-real-time manner. Therefore, So does not disclose or teach that selectively encrypted content is individually encrypted for delivery during a VOD session, which is the construction of an encrypted stream in real-time for delivery in real-time.

Additionally, claim 30 calls for routing the stream and a second encryption device for encryption. The Examiner has erred in not providing guidance as to where such claim features can be found in So.

3) Conclusion

Appellant respectfully submits that the Examiner has failed in presenting a prima facie case of obviousness with regard to the claims in Group 6. The arguments presented above regarding Claim Group 1 are equally applicable. The Examiner erred in not properly determining the scope and contents of the prior art as required by inquiry 1, maintaining that the So reference teaches real-time encryption of content when the reference as a whole actually teaches against real-time encryption of content. The Examiner also erred in not properly ascertaining the differences between the prior art and the claims in issue as required by inquiry 2, as shown above, the So reference teaches against real-time encryption of content and this feature is clearly recited in the claims of Group 6.

Hence, the Examiner has not supplied an "articulated reasoning" for the rejection of the claims in claim Group 3 per *In re Kahn*, supra. Additionally, the Examiner has not provided a disclosure for additional claim elements as recited above within the So reference or an articulated reasoning as to why any such disclosure teaches the additional claim elements. The Appellant asserts that there is no disclosure or teaching within the So reference for the claim elements recited in Claim Group 6.

Appellant respectfully submits that the claims of Group 6 are allowable for at least these reasons and requests reversal of the rejections.

Concluding Remarks

In view of the above arguments, it is submitted that the Examiner has erred and failed to establish *prima facie* unpatentability of any of the claims in Claim Groups 1-6. Accordingly, it is submitted that all claims are allowable. The undersigned respectfully requests that the Board Reverse of all rejections and pass the present application to allowance.

Respectfully submitted,

/Jerry A. Miller 30779/
Jerry A. Miller
Registration No. 30,779

Dated: 9/18/2007

Please Send Correspondence to:
Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606
Phone: (919) 816-9981
Fax: (919) 816-9982
Customer Number 24337

CLAIMS APPENDIX

1. (Previously Presented) A Video On Demand (VOD) method that provides session based selective encryption, comprising:

processing content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted;

storing the first portions;

storing second portions;

receiving a request for delivery of the content from a subscriber terminal to initiate a VOD session;

determining if the subscriber terminal has decryption capabilities associated with a first decryption method or a second decryption method;

if the request is from a subscriber terminal having decryption capabilities associated with the first decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the first decryption method to initiate a VOD session:

routing the first portions to a first encryption device that encrypts content for decryption under the first encryption method, to provide encryption of the first portions for the VOD session;

routing the second portions around the first encryption device;

encrypting neither the first nor the second portions using a second encryption device that encrypts content for decryption under the second decryption method for the VOD session;

encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions; and

if the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method:

routing the first portions to a second encryption device that encrypts content for decryption under the second encryption method, to provide encryption of the first portions for the VOD session;

routing the second portions around the second encryption device;

encrypting neither the first nor the second portions using the first encryption device that encrypts content for decryption under the first decryption method for the VOD session;

encrypting the first portions using the second encryption process at the second encryption device to produce encrypted first portions; and

assembling a stream of selectively encrypted content from the encrypted first portions and the second portions to produce a selectively encrypted stream of content that is individually encrypted for delivery during the VOD session.

2. (Original) The VOD method according to claim 1, wherein the first portions are stored in a first file and the second portions are stored in a second file.

3. (Original) The VOD method according to claim 2, wherein the first and second files are stored in a VOD server.

4. (Original) The VOD method according to claim 1, further comprising streaming the selectively encrypted content to the terminal.

5. (Previously Presented) The VOD method according to claim 1, wherein the first decryption method comprises a non-legacy encryption method.

6. (Original) The VOD method according to claim 1, wherein the assembled stream is passed through a second encryption device that is not provisioned to carry out encryption processing on the stream.

7. (Canceled)

8. (Previously Presented) The VOD method according to claim 1, wherein the second decryption method comprises a non-legacy encryption method.

9. (Original) The VOD method according to claim 1, carried out under control of a programmed processor.

10. (Original) computer readable storage medium storing instructions which, when executed on a programmed processor, carry out a process according to claim 1.

11. (Previously Presented) A Video On Demand (VOD) method that provides session based selective encryption, comprising:

processing content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted;

storing the first portions;

storing second portions;

receiving a request for delivery of the content from a subscriber terminal to initiate a VOD session;

determining if the subscriber terminal has decryption capabilities associated with a first decryption method or a second decryption method;

if the request is from a subscriber terminal having decryption capabilities associated with the first decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the first decryption method to initiate a VOD session:

routing the first portions to a first encryption device that encrypts content for decryption under the first encryption method, to provide encryption of the first portions for the VOD session;

routing the second portions around the first encryption device;

encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions; and

assembling a stream of selectively encrypted content from the encrypted first portions and the second portions to produce a selectively encrypted stream of content that is individually encrypted for delivery during the VOD session;

if the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method, but instead the request is from a terminal having decryption capabilities associated with the second decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the second decryption method to initiate a VOD session:

assembling a stream of content from the first portion and the second portion;

routing the stream to the second encryption device; and

encrypting the first portions using the second encryption device to produce an encrypted stream of content that is individually encrypted for delivery during the VOD session.

12. (Previously Presented) The VOD method according to claim 11, wherein the first and second portions are stored in a VOD server.

13. (Original) The VOD method according to claim 11, further comprising sending the selectively encrypted content to the terminal.

14. (Previously Presented) The VOD method according to claim 11, wherein the second decryption method comprises a legacy encryption method.

15. (Previously Presented) The VOD method according to claim 11, wherein the first decryption method comprises a non-legacy encryption method.

16. (Original) The VOD method according to claim 11, carried out under control of a programmed processor.

17. (Original) computer readable storage medium storing instructions which, when executed on a programmed processor, carry out a process according to claim 11.

18. (Currently Amended) A Video On Demand (VOD) server arrangement that provides session based encryption, comprising:

means for receiving content from a selective encryption processor that processes content to be delivered in a VOD method by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted;

a router;

a first encryption device;

a second encryption device;

at least one computer readable storage device;

a processor that:

stores the first and second portions in the at least one computer readable storage device;

receives a request for delivery of the VOD content as a VOD session, the request being from a subscriber terminal having decryption capabilities associated with either a first decryption method or a second decryption method;

determines if the request is from a terminal having decryption capabilities associated with the first decryption method or the second decryption method;

if the request is from a terminal having decryption capabilities associated with the first decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the first decryption method to initiate a VOD session:

the processor instructs the router to route the first portions to the first encryption device and not the second encryption device, and

routes the second portions around the first encryption device and around the second encryption device;

wherein, the first encryption device encrypts the first portions using a first encryption process to produce encrypted first portions;

if the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method:

routing the first portions to the second encryption device that encrypts content for decryption under the second encryption method, to provide encryption of the first portions for the VOD session;

routing the second portions around the second encryption device;

encrypting neither the first nor the second portions using the first encryption device that encrypts content for decryption under the first decryption method for the VOD session;

encrypting the first portions using the second encryption process at the second encryption device to produce encrypted first portions; and

means for assembling a stream of selectively encrypted content from the encrypted first portions and the second portions.

19. (Previously Presented) The server arrangement according to claim 18, wherein:

if the request is not from a subscriber terminal having decryption capabilities associated with the first decryption method, but instead the request is from a terminal having decryption capabilities associated with the second decryption method, then for each such request from a subscriber terminal having decryption capabilities associated with the second decryption method to initiate a VOD session:

the means for assembling assembles a stream of content from the first portion and the second portion;

the processor instructs the first router to route the stream to a second encryption device; and:

wherein the second encryption device encrypts the first portions using a second encryption process to produce a selectively encrypted stream.

20. (Original) The VOD server according to claim 18, wherein the first portions are stored in a first file and the second portions are stored in a second file.

21. (Original) The VOD server according to claim 18, further comprising means for streaming the selectively encrypted content to the terminal.

22. (Original) The VOD server according to claim 18, wherein the first encryption device encrypts using a legacy encryption method.

23. (Original) The VOD server according to claim 19, wherein the second encryption device encrypts using a non-legacy encryption method.

24. (Previously Presented) A Video On Demand (VOD) method that provides session based encryption, comprising:

receiving a request for delivery of content from a subscriber terminal;

retrieving the content from a storage medium;

processing the retrieved content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted;

determining if the request is from a subscriber terminal having decryption capabilities associated with a first decryption method or a second decryption method;

for each request from a subscriber terminal having decryption capabilities associated with the first decryption method to initiate a VOD session:

routing the first portions to a first encryption device;

routing the second portions around the first encryption device;

encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions; and

assembling a stream of selectively encrypted content from the encrypted first portions and the second portions to produce a selectively encrypted stream of content that is individually encrypted for delivery during the VOD session.

25. (Original) The VOD method according to claim 24, wherein the first portions and the second portions are stored in a computer readable file.

26. (Original) The VOD method according to claim 25, wherein the computer readable file is stored in a VOD server.

27. (Original) The VOD method according to claim 25, further comprising streaming the selectively encrypted content to the terminal.

28. (Original) The VOD method according to claim 25, wherein the first decryption method comprises a legacy encryption method.

29. (Original) The VOD method according to claim 25, wherein the assembled stream is passed through a second encryption device that is not provisioned to carry out encryption processing on the stream.

30. (Previously Presented) The VOD method according to claim 25, further comprising:

for each request from a subscriber terminal having decryption capabilities associated with the second decryption method to initiate a VOD session:

assembling a stream of content from the first portion and the second portion;

routing the stream to a second encryption device; and

encrypting the first portions using a second encryption process at the second encryption device to produce a selectively encrypted stream of content that is individually encrypted for delivery during the VOD session.

31. (Original) The VOD method according to claim 25, wherein the second decryption method comprises a non-legacy encryption method.

32. (Original) The VOD method according to claim 25, carried out under control of a programmed processor.

33. (Original) A computer readable storage medium storing instructions which, when executed on a programmed processor, carry out a process according to claim 25.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None